UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

CHAD ROSENTHAL, on behalf of himself and on behalf of all other similarly situated individuals,

Plaintiff,

v.

DXC TECHNOLOGY SERVICES, LLC,

Defendant.

Case No. 1:25-cv-327

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Chad Rosenthal ("Plaintiff"), individually and on behalf of all other similarly situated individuals (the "Class" or "Class Members," as defined below), by and through his undersigned counsel, files this Class Action Complaint against DXC Technology Services, LLC ("DXC" or "Defendant") and alleges the following based on personal knowledge of facts, upon information and belief, and based on the investigation of his counsel as to all other matters.

I. NATURE OF THE ACTION

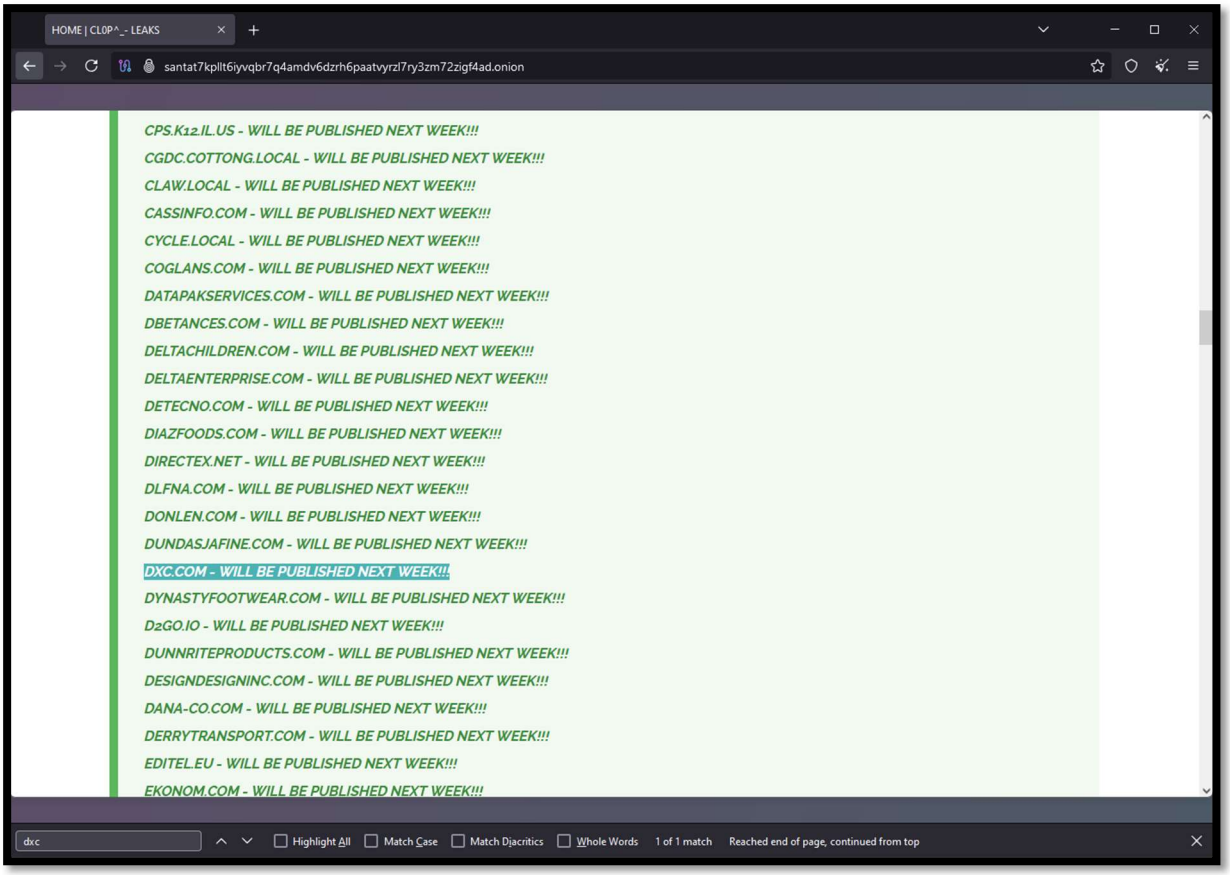
1. Plaintiff brings this class action lawsuit against Defendant for its negligent failure to protect and safeguard Plaintiff's and the Class's highly sensitive personally identifiable information ("PII"). As a result of Defendant's negligence and insufficient data security, cybercriminals easily infiltrated Defendant's inadequately protected servers and stole the PII of Plaintiff and the Class. Now, Plaintiff's and the Class's PII is in the hands of cybercriminals who will undoubtedly use their PII for nefarious purposes for the rest of their lives.

2. DXC is an IT solutions and consulting company with 130,000 employees worldwide.[1] DXC Technology provides a diverse range of services including analytics, consulting, application development, and security across more than 70 countries.[2] DXC was established through the merger of CSC and the Enterprise Services business of Hewlett Packard Enterprise.[3]

3. On or around February 10, 2025, notorious ransomware group—Cl0p ("Clop")—took responsibility for a ransomware attack waged against DXC (the "Data Breach" or "Breach").[4]

[IMAGE ON NEXT PAGE]

[1] https://cybernews.com/cybercrime/chicago-schools-dxc-technology-cl0p-ransomware/.
[2] https://www.redpacketsecurity.com/clop-ransomware-victim-dxc-com/.
[3] *Id.*
[4] Id.; https://cybernews.com/cybercrime/chicago-schools-dxc-technology-cl0p-ransomware/.



4. Clop is the same ransomware group that perpetrated the extensive MOVEit heist in 2023.[5]

5. Apparently the MOVEit heist was not enough; DXC was one of 47 companies listed as Clop's latest victims on Clop's data leak dark web site.[6]

6. Clop claimed DXC and the other companies breached "ignored" the Clop's notice and have not contacted the gang to negotiate a ransom payment.[7]

[5] https://cybernews.com/cybercrime/chicago-schools-dxc-technology-cl0p-ransomware/.
[6] *Id.*
[7] *Id.*

7. Clop distinguishes itself from other ransomware gangs through its unique approach to communication.[8] Rather than reaching out to affected companies directly, the gang posts a message on its dark web platform, prompting victims to initiate contact.[9]

8. Clop utilizes the ransomware-as-a-service (RaaS) model, allowing affiliates to use its ransomware software in exchange for a predetermined share of the ransom.[10]

9. Clop uses a "double-extortion" tactic, in which it both encrypts and steals victim data.[11] If the ransom is not paid, Clop not only refuses to restore access but also publishes the exfiltrated data on its leak site.[12]

10. At this time, it is unclear how many victims there are.

11. Upon information and belief, the PII stolen by Clop in the Data Breach includes highly sensitive private information such as: names; dates of birth; addresses; Social Security numbers; driver's license numbers; financial information (e.g., account number, credit or debit card number); medical information; and/or health insurance information (collectively, "Private Information").

12. Despite Clop publicly acknowledging the Data Breach, DXC has yet to inform victims of the Data Breach.

13. Due to Defendant's negligence, cybercriminals have stolen and obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

---

[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*

14. Now, and for the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information. Even those Class Members who have yet to experience identity theft have to spend time responding to the Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their Private Information, loss of privacy, and/or additional damages as described below.

15. In sum, Plaintiff and the Class will face an imminent risk of fraud and identity theft for the rest of their lives because (i) Defendant failed to protect Plaintiff's and the Class's PII, allowing a massive and preventable Data Breach to occur; (ii) the cybercriminals who perpetrated the Breach stole Private Information that they will leak on the dark web (if they have not already); (iii) Defendant has failed to provide any assurance that it paid a ransom demand to prevent Plaintiff's and the Class's data from being released on the dark web; and (iv) Defendant has failed to notify victims of the Data Breach that their PII is in the hands of cybercriminals.

16. Plaintiff brings this action individually and on behalf of the Class, seeking compensatory damages, punitive damages, nominal damages, restitution, and injunctive and declaratory relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

17. Plaintiff **Chad Rosenthal** is an individual domiciled in Irving, Texas. Upon information and belief, Plaintiff is a victim of the Data Breach, and his Private Information was

stolen by Clop.

18. Defendant **DXC Technology Services LLC** is a Delaware limited liability company. DXC is headquartered in Ashburn, Virginia and has members and managers who reside in this District. DXC's principal place of business is located at 20408 Bashan Dr., STE 231, Ashburn, VA, 20147-5553. DXC's registered agent is Corporate Creations Network Inc., located at 425 W Washington St Ste 4, Suffolk, VA, 23434-5320.

III. JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than one hundred putative Class Members, and minimal diversity exists because many putative Class Members are citizens of a different state than Defendant.

20. This Court has personal jurisdiction over Defendant because Defendant is registered to do business in the Commonwealth of Virginia and has members and managers residing in this District; has its principal place of business in this District; conducts substantial business in this District through its headquarters, offices, and affiliates; engaged in the conduct at issue here in this District; and/or otherwise has substantial contacts with this District and purposely availed itself to the Courts in this District.

21. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District.

IV. FACTUAL ALLEGATIONS

A. Defendant and its Collection of Plaintiff's and the Class's PII.

22. "DXC Technology is a leading global IT services company that specializes in helping businesses drive digital transformation. Originally formed as a result of the merger between CSC and the Enterprise Services business of Hewlett Packard Enterprise (HPE) in 2017, DXC provides end-to-end IT services in over 70 countries, catering to various industries and sectors. It offers a broad range of services including analytics, consulting, application development, and security."[13]

23. According to Defendant, DXC "helps global companies run their mission-critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. The world's largest companies and public sector organizations trust DXC to deploy services to drive new levels of performance, competitiveness, and customer experience across their IT estates."[14]

24. Ironically, DXC touts itself as a leader in cyber risk management.[15]

25. DXC claims it helps businesses "assess risk and proactively address all facets of [their] security environment, from threat intelligence to compliance" while also "leverage[ing] proven methodologies, intelligent automation and industry-leading partners to tailor security solutions to [] unique business needs."[16]

[13] https://www.ransomware.live/id/ZHhjLmNvbUBjbG9w.
[14] https://dxc.com/us/en/about-us/values.
[15] https://dxc.com/us/en/offerings/security.
[16] *Id.*

26. On February 4, 2025, DXC reported "[t]otal revenue of $3.23 billion[.]"[17] In other words, Defendant could have afforded to implement adequate data security prior to the Breach but deliberately chose not to.

27. In the ordinary course of business, Defendant receives the PII of individuals, such as Plaintiff and the Class, from the entities and individuals that utilize Defendant's services. Defendant also receives the PII of its current and former employees.

28. Defendant obtains, collects, uses, and derives a benefit from the PII of Plaintiff's and Class Members. Defendant uses the PII it collects to provide services, making a profit therefrom. Defendant would not be able to obtain revenue if not for the acceptance and use of Plaintiff's and the Class's PII.

29. By collecting Plaintiff's and the Class's PII, Defendant assumed legal and equitable duties to Plaintiff and the Class to protect and safeguard their PII from unauthorized access and intrusion.

30. Defendant recognizes this duty and makes the following claim on its website regarding its protection of sensitive data:

> At DXC Technology (DXC) our commitment to privacy goes beyond the minimum legal and regulatory requirements. We strive for best-in-class data protection and privacy management; this requires a sound data privacy governance structure and an effective data privacy compliance and best practices program. With these measures, DXC aims to comply with ever-changing and increasingly complex regulatory standards; meet contractual privacy obligations; and build trust with our employees, customers, business partners and other stakeholders.[18]

[17] https://investors.dxc.com/investor-news/news-details/2025/DXC-Technology-Reports-Third-Quarter-Fiscal-Year-2025-Results/.
[18] https://dxc.com/us/en/privacy.

31. Defendant's assurances of maintaining high standards of cybersecurity make it evident that Defendant recognized it had a duty to use reasonable measures to protect the PII that it collected and maintained.

32. Defendant violated its own privacy statement and failed to adopt reasonable and appropriate security practices and procedures including administrative, physical security, and technical controls to safeguard Plaintiff's and the Class's Private Information.

33. As a result, Plaintiff's and Class Members' PII was accessed and stolen from Defendant's inadequately secured data systems in a massive and preventable Data Breach orchestrated by Clop.

B. Defendant's Massive and Preventable Data Breach.

34. In or around February 2025, DXC was one of 47 organizations who networks were breached by Clop.[19]

35. Clop posted DXC to its data leak site on the dark web after DXC "ignored" Clop.[20]

36. DXC has yet to publicly acknowledge the Data Breach and provide notice of the Data Breach to the victims.

37. When a ransomware gang such as Clop attacks a corporate target, they first steal data from the network and then encrypt files.[21] This stolen data is used as leverage in double-extortion attacks, warning victims that the data will be leaked if a ransom is not paid.[22]

38. When victims try to open a damaged file, they see a ransom note. This note tells

[19] https://www.scworld.com/brief/dozens-of-orgs-claimed-to-be-hacked-by-cl0p-ransomware.
[20] *Id.*
[21] https://www.bleepingcomputer.com/news/security/clop-now-leaks-data-stolen-in-moveit-attacks-on-clearweb-sites/
[22] *Id.*

them their files are encrypted and explains how to pay the ransom, often in Bitcoin or another cryptocurrency.[23]

39. For the companies that do not pay Clop's ransom demand, Clop will "leak" the data on the dark web for anyone to use and abuse how they please.[24]

40. Ransomware data leak sites are usually located on the Tor network on the dark web as it makes it harder for the website to be taken down or for law enforcement to seize their infrastructure.[25]

41. However, Clop has also been known to post data on the clear web as well, allowing anyone with internet access to access and download PII from the web.[26]

42. Clop is known for stealing PII such as names; dates of birth; addresses; Social Security numbers; driver's license numbers; financial information (e.g., account number, credit or debit card number); medical information; and health insurance information.[27] Upon information and belief, Clop stole this exact information from DXC because that is the *modus operandi* of threat actors like Clop.

43. Specialists do not recommend the victims affected by ransomware attacks pay the threat actors, no matter what the cost is.[28] Researches reveal that after ransomware hackers receive their payment, they ignore the victims. This leaves no chance to get the encrypted data back.[29]

44. "One of the biggest issues with paying a ransom is that you're gambling that

---

[23] https://heimdalsecurity.com/blog/clop-ransomware-overview/.
[24] Id.
[25]https://www.bleepingcomputer.com/news/security/clop-now-leaks-data-stolen-in-moveit-attacks-on-clearweb-sites/.
[26] *Id.*
[27] *See* https://www.bleepingcomputer.com/news/security/clop-ransomware-is-now-extorting-66-cleo-data-theft-victims/.
[28] https://heimdalsecurity.com/blog/clop-ransomware-overview/.
[29] *Id.*

hackers will keep to their word and restore systems. Unfortunately, when you're dealing with criminals, there's no guarantee. In fact, it's estimated that as many as 92 percent of firms fail to recover all of their data, with nearly a third losing at least half."[30]

45. "If the hackers have successfully exfiltrated data as part of their attack, there's also no way of knowing what they'll do with this, even if a ransom is paid. Many cybergangs make additional revenue by selling the data on the dark web, especially if it contains valuable intellectual property or customer data. This can cause significant long term problems for the organization in terms of lost competitiveness and reputational damage."[31]

46. DXC has yet to publicly recognize the severity of the Data Breach and the imminent risk of harm Plaintiff and the Class face.

47. All in all, Defendant failed to take the necessary precautions required to safeguard and protect Plaintiff's and Class Members' PII from unauthorized access and exploitation. Clop has been around for years and there are many simple preventative measures DXC could have taken to prevent the Data Breach, but it failed to do so.

48. Defendant's actions represent a flagrant disregard of the rights of Plaintiff and the Class, both as to privacy and property.

C. Cybercriminals Will Use Plaintiff's and the Class's PII to Defraud Them.

49. PII is of great value to hackers and cybercriminals, and the data stolen in the Data Breach can and will be used in a variety of ways by criminals to exploit Plaintiff and the Class Members and to profit off their misfortune.

[30] https://www.blackfog.com/should-you-pay-a-ransomware-demand/.
[31] *Id.*

50. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[32]

51. For example, with the PII stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[33] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and the Class Members.

52. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[34]
>
> [Emphasis added.]

---

[32] *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[33] *See, e.g.*, Christine DiGangi, *What Can You Do with a Stolen Social Security Number*, CREDIT.COM (June 29, 2020), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[34] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

53. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[35]

54. This was a financially motivated Breach, as the only reason the cybercriminals go through the trouble of running targeted cyberattacks against companies like Defendant is to get ransom money and/or information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein.

55. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[36]

56. "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[37]

57. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, ***they will use it***.[38]

58. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the

---

[35] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, available at https://www.gao.gov/products/gao-07-737.

[36] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web* (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[37] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[38] Ari Lazarus, *How fast will identity thieves use stolen info?*, MILITARY CONSUMER (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info.

> Web, fraudulent use of that information ***may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[39]

59. For instance, with a stolen social security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[40]

60. With this Data Breach, identity thieves have already started to prey on the Defendant Data Breach victims, and we can anticipate that this will continue.

61. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[41]

62. Defendant's offer of one year of identity monitoring to Plaintiff and the Class is woefully inadequate and will not fully protect Plaintiff from the damages and harm caused by its failures.

63. The full scope of the harm has yet to be realized. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used.

64. Plaintiff and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to Defendant's gross negligence.

---

[39] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* GAO (July 5, 2007), available at https://www.gao.gov/products/gao-07-737.

[40] *See, e.g.*, Christine DiGangi, *What Can You Do with a Stolen Social Security Number*, CREDIT.COM (June 29, 2020), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[41] *Guide for Assisting Identity Theft Victims*, FEDERAL TRADE COMMISSION (Sept. 2013), *available at* https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.

65. Furthermore, identity monitoring only alerts someone to the fact that they have ***already been the victim of identity theft*** (*i.e.*, fraudulent acquisition and use of another person's PII)—it does not prevent identity theft.[42] Nor can an identity monitoring service remove personal information from the dark web.[43]

66. "The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[44]

67. As a direct and proximate result of the Data Breach, Plaintiff and the Class have been damaged and have been placed at an imminent, immediate, and continuing increased risk of harm from continued fraud and identity theft. Plaintiff and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

68. Even more seriously is the identity restoration that Plaintiff and other Class Members must go through, which can include spending countless hours filing police reports, filling out IRS forms, Federal Trade Commission checklists, Department of Motor Vehicle driver's license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiff and the Class must take.

---

[42] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017, 9:00 AM), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html.
[43] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know.
[44] *Id.*

69. Plaintiff and the Class have or will experience the following concrete and particularized harms for which they are entitled to compensation, including:

a. Actual identity theft;

b. Trespass, damage to, and theft of their personal property including PII;

c. Improper disclosure of their PII;

d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their PII;

f. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class Members' Private Information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their PII; and/or

k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

70. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected from further

breaches by the implementation of industry standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiff's and the Class's Private Information.

71. Plaintiff and Class Members also have an interest in ensuring that their Private Information that was provided to Defendant is removed from all Defendant servers, systems, and files.

72. Defendant has yet to acknowledge the harm caused by the Data Breach.

73. As a result of Defendant's negligence, Plaintiff and the Class are desperately trying to mitigate the damage that Defendant has caused them.

74. Given the kind of Private Information Defendant made accessible to hackers, however, Plaintiff and the Class are certain to incur additional damages. Because identity thieves have their PII, Plaintiff and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[45]

75. None of this should have happened because the Data Breach was entirely preventable.

D. Defendant was Aware of the Risk of Cyberattacks.

76. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some

[45] *What happens if I change my Social Security number*, LEXINGTON LAW (Aug. 10, 2022), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

of the biggest cybersecurity breaches: Target,[46] Yahoo,[47] Marriott International,[48] Chipotle, Chili's, Arby's,[49] and others.[50]

77. The number of data breach victims has surpassed 1 billion for the first half of 2024, according to the Identity Theft Resource Center.[51]

78. Defendant should certainly have been aware, and indeed was aware, that it was at risk of a data breach that could expose the PII that it collected and maintained.

79. Defendant was clearly aware of the risks it was taking and the harm that could result from inadequate data security but threw caution to the wind.

E. Defendant Could Have Prevented the Data Breach.

80. Data breaches are preventable.[52] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate

---

[46] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[47] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[48] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/ (last visited Oct. 9, 2023).

[49] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018, 12:58 PM), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[50] *See, e.g.*, Michael Hill and Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Nov. 8, 2022), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[51] https://www.usatoday.com/story/money/2024/07/18/data-breach-what-to-do/74441060007/.

[52] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012), available at https://lawcat.berkeley.edu/record/394088.

security solutions."[53] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[54]

81. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[55]

82. In a data breach like this, many failures laid the groundwork for the Breach.

83. The FTC has published guidelines that establish reasonable data security practices for businesses.

84. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[56]

85. The FTC guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems.

86. The FTC guidelines also recommend that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating

---

[53] *Id.* at 17.
[54] *Id.* at 28.
[55] *Id.*
[56] *Protecting Personal Information: A Guide for Business*, FTC, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

87. According to information and belief, Defendant failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines.

88. Upon information and belief, Defendant also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

89. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[57]

90. To prevent and detect malware attacks, including the malware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy

[57] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or

compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[58]

91. Further, to prevent and detect malware attacks, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….
- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious

[58] *Id.* at 3–4.

website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….
- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[59]

92. In addition, to prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privileged credentials
- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise;
- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
- **Build credential hygiene**
  - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

[59] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at https://www.cisa.gov/news-events/news/protecting-against-ransomware.

- **Apply principle of least-privilege**
    - Monitor for adversarial activities
    - Hunt for brute force attempts
    - Monitor for cleanup of Event Logs
    - Analyze logon events
- **Harden infrastructure**
    - Use Windows Defender Firewall
    - Enable tamper protection
    - Enable cloud-delivered protection
    - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[60]

93. Given that Defendant was storing the PII of more than thousands of individuals, Defendant could have and should have implemented all of the above measures to prevent and detect cyberattacks.

94. Specifically, among other failures, Defendant had far too much confidential unencrypted information held on its systems. Such PII should have been segregated into an encrypted system.[61]

95. Moreover, it is a well-established industry standard practice for a business to dispose of confidential PII once it is no longer needed.

---

[60] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

[61] *See, e.g.,* Adnan Raja, *How to Safeguard Your Business Data with Encryption*, FORTRA (Aug. 14, 2018), https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.

96. The FTC, among others, has repeatedly emphasized the importance of disposing unnecessary PII, saying simply: "Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not on your system, it can't be stolen by hackers."[62] Defendant, rather than following this basic standard of care, kept thousands of individuals' unencrypted PII indefinitely.

97. In sum, the Data Breach could have readily been prevented through the use of industry standard network segmentation and encryption of all PII.

98. Further, the scope of the Data Breach could have been dramatically reduced had Defendant utilized proper record retention and destruction practices.

F. Plaintiff's Individual Experience

Plaintiff Chad Rosenthal

99. Plaintiff Rosenthal is a former employee of Defendant.

100. Upon information and Plaintiff's Private Information was stolen from Defendant's systems in the Data Breach.

101. Defendant was in possession of Plaintiff's Private Information before, during, and after the Data Breach.

102. Because of the Data Breach, there is no doubt Plaintiff Rosenthal's highly confidential Private Information is in the hands of cybercriminals. Reason being, Clop confirmed it stole data from Defendant's systems on its dark web leak site. As such, Plaintiff Rosenthal and the Class are at an imminent risk of identity theft and fraud.

---

[62] *Protecting Personal Information: A Guide for Business*, FTC, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf, at p. 6.

103. As a result of the Data Breach, Plaintiff Rosenthal has already expended hours of his time and has suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including investigating the Data Breach, investigating how best to ensure that he is protected from identity theft, and reviewing account statements, credit reports, and/or other information.

104. Plaintiff Rosenthal places significant value on the security of his Private Information and does not readily disclose it. Plaintiff Rosenthal has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

105. Plaintiff Rosenthal has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information compromised by the Data Breach.

106. Plaintiff Rosenthal has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiff's and the Class's Private Information will be wholly unprotected and at-risk of future data breaches.

107. Plaintiff Rosenthal has suffered injuries directly and proximately caused by the Data Breach, including: (i) theft of his valuable Private Information; (ii) the imminent and certain impending injury flowing from anticipated fraud and identity theft posed by his Private Information being placed in the hands of cybercriminals; (iii) damages to and diminution in value of his Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between

what Plaintiff Rosenthal should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect his Private Information; and (v) continued risk to his Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

V. CLASS ACTION ALLEGATIONS

108. Plaintiff incorporates by reference all preceding paragraphs as if fully restated here.

109. Plaintiff brings this action against Defendant on behalf of himself and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of a nationwide class (the "Class") defined as follows:

> **All persons whose data was accessed or stolen in the Data Breach.**

110. Excluded from the Class is Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

111. Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

112. Plaintiff anticipates the issuance of notice setting forth the subject and nature of the instant action to the proposed Class. Upon information and belief, Defendant's own business records or electronic media can be utilized for the notice process.

113. The proposed Class meets the requirements of Federal Rule of Civil Procedure 23.

114. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable.

115. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Defendant's uniform misconduct. Defendant's inadequate data security gave rise to Plaintiff's claims and are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive PII compromised in the same way by the same conduct of Defendant.

116. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and their counsel.

117. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

118. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's PII;

c. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their PII, and whether it breached this duty;

d. Whether Defendant breached its duties to Plaintiff and the Class;

e. Whether Defendant failed to provide adequate cyber security;

f. Whether Defendant knew or should have known that its computer and network security systems were vulnerable to cyber-attacks;

g. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its company network;

h. Whether Defendant was negligent in permitting unencrypted PII off vast numbers of individuals to be stored within its network;

i. Whether Defendant was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach;

j. Whether Defendant breached implied contractual duties to Plaintiff and the Class to use reasonable care in protecting their PII;

k. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most

expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

l. Whether Defendant continues to breach duties to Plaintiff and the Class;

m. Whether Plaintiff and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

n. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief; and

o. Whether Defendant's actions alleged herein constitute gross negligence, and whether Plaintiff and Class Members are entitled to punitive damages.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

119. Plaintiff incorporates paragraphs 1–118 as though fully set forth herein.

120. Defendant solicited, gathered, and stored the PII of Plaintiff and Class Members.

121. Upon accepting and storing the PII of Plaintiff and Class members on its computer systems and networks, Defendant undertook and owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiff and the Class from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

122. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class members could and would suffer if the PII was wrongfully disclosed. Plaintiff and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class members had no ability to protect their PII that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiff and the Class.

123. Because of this special relationship, Defendant required Plaintiff and Class members to provide their PII, including names, Social Security numbers, and other PII.

124. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiff and Class members in its possession was only used for the provided purpose and that Defendant would destroy any PII that it was not required to maintain.

125. As part of this special relationship, Defendant had a duty to perform with skill, care, and reasonable expedience and faithfulness.

126. Through Defendant's acts and omissions, including Defendant's failure to provide adequate data security, its failure to protect Plaintiff's and Class members' PII from being foreseeably accessed, and its improper retention of PII it was not required to maintain, Defendant negligently failed to observe and perform its duty.

127. Plaintiff and Class members did not receive the benefit of the bargain with Defendant, because providing their PII was in exchange for Defendant's implied agreement to secure and keep it safe and to delete it once no longer required.

128. Defendant was aware of the fact that cybercriminals routinely target large business entities through cyberattacks in an attempt to steal customer and employee PII. In other words, Defendant knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures.

129. Defendant owed Plaintiff and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard or delete such data and providing notification to Plaintiff and the Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

130. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

131. Defendant had duties to protect and safeguard the PII of Plaintiff and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive PII. Additional duties that Defendant owed Plaintiff and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class members' PII was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiff's and Class members' PII in its possession by using reasonable and adequate security procedures and systems;

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its networks and servers; and

d. To promptly notify Plaintiff and Class members of any data breach, security incident, or intrusion that affected or may have affected their PII.

132. Plaintiff and the Class were the intended beneficiaries of Defendant's duties, creating a special relationship between them and Defendant. Defendant was in a position to ensure that its systems were sufficient to protect the PII that Plaintiff and the Class had entrusted to it.

133. Plaintiff's injuries and damages, as described herein, are a reasonably certain consequence of Defendant's negligence and breach of its duties.

134. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class members' PII. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, and protecting the PII in its possession;

b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to consistently enforce security policies aimed at protecting Plaintiff and the Class's PII;

d. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

e. Failing to promptly notify Plaintiff and Class members of the Data Breach that affected their PII.

135. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent considering the foreseeable risks and known threats.

136. As a direct and proximate result of Defendant's negligent conduct, including but not limited to its failure to implement and maintain reasonable data security practices and procedures as described above, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

137. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the PII of Plaintiff and Class members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiff and Class members while it was within Defendant's possession and control.

138. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class members, Defendant prevented Plaintiff and Class members from taking meaningful, proactive steps to securing their PII and mitigating damages.

139. Plaintiff and Class members could have taken actions earlier had they been timely notified of the Data Breach.

140. Plaintiff and Class members could have enrolled in credit monitoring, could have instituted credit freezes, and could have changed their passwords, among other things, had they been alerted to the Data Breach more quickly.

141. Plaintiff and Class members have suffered harm from the delay in notifying them of the Data Breach.

142. As a direct and proximate cause of Defendant's conduct, including but not limited to its failure to implement and maintain reasonable security practices and procedures, Plaintiff and Class members have suffered, as Plaintiff have, and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PII is used; (ii) the publication and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protections; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in Defendant's possession

and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of employees in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives. Thus, Plaintiff and the Class are entitled to damages in an amount to be proven at trial.

143. The damages Plaintiff and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's negligent conduct.

144. Plaintiff and the Class have suffered injury and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

145. Plaintiff incorporates paragraphs 1–118 as though fully set forth herein.

146. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant had a duty to Plaintiff and the Class to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiff and the Class.

147. The FTC Act prohibits "unfair practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

148. Defendant gathered and stored the PII of Plaintiff and the Class as part of their business which affects commerce.

149. Defendant violated the FTC Act by failing to use reasonable measures to protect the PII of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

150. Defendant breached its duties to Plaintiff and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiff's and Class members' PII, and by failing to provide prompt notice without reasonable delay.

151. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

152. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

153. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against.

154. Defendant breached its duties to Plaintiff and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class's PII.

155. Defendant breached its duties to Plaintiff and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiff and the Class.

156. Defendant's violations of the FTC Act constitute negligence *per se*.

157. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

158. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

159. Plaintiff and the Class have suffered injury and are entitled to damages in amounts to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

160. Plaintiff incorporates paragraphs 1–118 as though fully set forth herein.

161. Plaintiff and Class Members were required deliver their PII to Defendant as part of the process of obtaining employment services provided by Defendant.

162. Defendant solicited, offered, and invited Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

163. Defendant accepted possession of Plaintiff's and Class Members' PII for the purpose of providing services to Plaintiff and Class Members.

164. Plaintiff and the Class entrusted their PII to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

165. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations (including FTC guidelines on data security) and were consistent with industry standards.

166. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take

reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

167. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

168. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it Defendant promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

169. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

170. Plaintiff and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

171. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

172. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

173. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or Defendant terms.

174. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

175. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

176. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of PII and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

177. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to

further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

178. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

179. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

180. Plaintiff incorporates paragraphs 1–118 as though fully set forth herein.

181. Plaintiff alleges this claim in the alternative to his breach of contract claim.

182. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiff's retained data and commercialized and used Plaintiff's and Class Members' PII for business purposes.

183. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiff and Class Members.

184. As such, a portion of the payments made for the benefit of or on behalf of Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

185. Defendant failed to secure Plaintiff's and Class Members' Private Information and,

therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

186. Defendant acquired the PII through inequitable means as it failed to disclose the inadequate data security practices previously alleged. If Plaintiff and Class Members had known that Defendant would not fund adequate data security practices, procedures, and protocols to sufficiently monitor, supervise, and secure their PII, they would not have entrusted their Private Information to Defendant or obtained services from Defendant's clients.

187. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to their own benefit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their PII.

188. Plaintiff and Class Members have no adequate remedy at law.

189. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

190. As a direct and proximate result of Defendant's conduct, Plaintiff and other Class Members, have suffered actual harm in the form of experiencing specific acts of fraudulent activity and other attempts of fraud that required Plaintiff' efforts to prevent from succeeding.

191. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Defendant and all other relief allowed by law.

FIFTH CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiff and the Class)

192. Plaintiff incorporates paragraphs 1–118 as though fully set forth herein.

193. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

194. As previously alleged, Plaintiff and members of the Class are entered into implied contracts with Defendant, which contracts required Defendant to provide adequate security for the PII collected from Plaintiff and the Class.

195. Defendant owed and still owes a duty of care to Plaintiff and Class members that require it to adequately secure Plaintiff's and Class members' PII.

196. Upon reason and belief, Defendant still possesses the PII of Plaintiff and the Class members.

197. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class members.

198. Since the Data Breach, Defendant has not yet announced any changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and go undetected and, thereby, prevent further attacks.

199. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

200. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and the members

of the Class. Further, Plaintiff and the members of the Class are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that led to such exposure.

201. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

202. Plaintiff and the Class, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment employee data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems

is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, customer data not necessary for their provisions of services;

f. Ordering that Defendant conduct regular database scanning and security checks; and

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff are proper representatives of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Class Action Complaint.

Dated: February 19, 2025

Respectfully submitted,

By: */s/ Lee A. Floyd*
Lee A. Floyd (VSB No. 88459)
Justin M. Sheldon (VSB No. 82632)
BREIT BINIAZAN, PC
2100 East Cary Street, Suite 310
Richmond, Virginia 23223
Telephone: (804) 351-9040
Facsimile: (804) 351-9170
Lee@bbtrial.com
Justin@bbtrial.com

William B. Federman, OBA No. 2853
(*pro hac vice* application forthcoming)
Kennedy M. Brian, OBA No. 34617
(*pro hac vice* application forthcoming)
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
T: (405) 235-1560
F: (405) 239-2112
E: wbf@federmanlaw.com
E: kpb@federmanlaw.com

Counsel for Plaintiff